Polo del Conocimiento

Pol. Con. (Edición núm. 16) Vol. 3, No 2
Febrero 2018, pp. 118-131
ISSN: 2550 - 682X
DOI: 10.23857/pc.v3i2.456

Recepción: 20 / 11 / 2017
Aceptación: 15 / 01 / 2018
Publicación: 21 / 02 / 2018

Ciencias de la computación

Artículo Científico

La Criptografía como elemento de la seguridad informática

Cryptography as an element of computer security

Criptografia como elemento de segurança de computadores

Baster L. Estupiñán-Ortiz [I]
basterl.estupinanor1@yahoo.com

Cristóbal C. Bone-Obando [II]
colonboneo@gmail.com

Correspondencia: basterl.estupinanor1@yahoo.com

I. Magister en Docencia y Desarrollo del Currículo, Ingeniero en Sistemas Informáticos, Profesor de Segunda Enseñanza Especialidad Física y Matemáticas, Docente de la Universidad Luis Vargas Torres de Esmeraldas, Esmeraldas, Ecuador.

II. Magister en Gerencia de Proyectos Educativos y Sociales, Magister en Docencia Mención Gestión en Desarrollo del Currículo, Doctor en Ciencias de la Educación Mención Investigación Educativa, Licenciado en Ciencias de la Educación Profesor de Segunda Enseñanza en la Especialización de Física y Matemática, Docente Universidad Técnica Luis Vargas Torres de Esmeraldas, Esmeraldas, Ecuador.

Resumen

La globalización de la economía ha exigido que las empresas implementen plataformas tecnológicas que soporten la nueva forma de hacer negocios. El uso de Internet para este fin, conlleva a que se desarrollen proyectos de seguridad informática que garanticen la integridad, disponibilidad y accesibilidad de la información. La creación de políticas de seguridad es una labor fundamental que involucra las personas, los procesos y los recursos de las compañías. Vale acotar, que hoy es imposible hablar de un sistema cien por cien seguros, sencillamente porque el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen riesgos: deben optar entre perder un negocio o arriesgarse a ser hackeadas. En este sentido, crear diferentes mecanismos, dirigidos a garantizar la confidencialidad y autenticidad de los documentos electrónicos, todo ello es parte de una nueva tecnología denominada Criptografía. Se aborda el tema de la seguridad informática, en específico las diversas variantes criptográficas: simétrica y asimétrica además de los elementos de la Seguridad Informática (PSI) como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Estos permiten a las compañías desarrollarse y mantenerse en su sector de negocios basándose en la norma ISO 17799.

Palabras claves: Criptografía, Seguridad, Informática, Transacciones, Electrónicas.

Abstract

The globalization of the economy has demanded that companies implement technological platforms that support the new way of doing business. The use of Internet for this purpose, leads to the development of computer security projects that guarantee the integrity, availability and accessibility of information. The creation of security policies is a fundamental task that involves the people, processes and resources of the companies. It is worth mentioning that today it is impossible to speak of a 100% insurance system, simply because the cost of total security is very high. That is why companies, in general, assume risks: they must choose between losing a business or risking being hacked. In this sense, create different mechanisms, aimed at ensuring the confidentiality and authenticity of electronic documents, all part of a new technology called Cryptography. The issue of computer security is addressed, specifically the various cryptographic variants: symmetric and asymmetric as well as the elements of Information Security (PSI) as an organizational tool to raise awareness among each member of an organization about the importance and sensitivity of information and critical services. These allow companies to develop and maintain their business sector based on ISO 17799.

Key words: Cryptography, Security, Computing, Transactions, Electronics.

Introducción.

El mundo digital se ha integrado en toda la sociedad de una forma vertiginosa, en nuestro diario vivir son más las personas que se apoyan en Internet para utilizar sus servicios y realizar sus actividades, enviar un correo electrónico, participar en un foro de discusión, tener una sesión de chat, comunicación de voz sobre ip, descargar música o el libro favorito, hacer publicidad, etc. Son algunas de las cosas más comunes. Sin embargo, el mundo de los negocios empresariales es aún más complejo y la gama de servicios nos presenta mayores alternativas. Las "transacciones" electrónicas nos permiten ahorrar tiempo y recursos, pagar los servicios públicos, transferir de una cuenta bancaria a otra, participar en una subasta para comprar un vehículo, pagar un boleto de avión etc. En todos estos ejemplos hay algo en común, el dinero, y cuando hablamos de tan escaso pero tan apreciado bien las empresas deben garantizar la implementación de políticas de seguridad informática. (DUSSÁN,2006)

Los que trabajan en el mundo empresarial, deben recibir instrucciones claras y definitivas que los ayuden a garantizar la seguridad de la información en el complejo mundo de los negocios. Cada vez encontramos más gerentes interesados en entender las reglas del negocio, entre ellas las referentes a las políticas de seguridad informática. El ofrecer productos o servicios a través de Internet sin tomar en cuenta la seguridad informática no sólo denota negligencia, sino que constituye una invitación para que ocurran incidentes de seguridad que podrían dañar severamente la reputación y afectar los ciclos del negocio. (DUSSÁN, 2006)

Las empresas han implementado un modelo de acceso a la información más abierto y a la vez más distribuido, lo cual redunda en beneficios tales como:

- Mayor productividad por empleado: Los empleados agilizan su trabajo, toman mejores decisiones y responden con rapidez a las cambiantes demandas del mercado en el que se mueven, al tener un acceso seguro a la información que necesitan desde cualquier lugar y en cualquier momento.
- Reducción de costos: Reduce los costos e incrementa la efectividad a través de las herramientas de colaboración y de la conectividad de red. (RODRÍGUEZ, 2000)
- Integración de los procesos de negocios: Incrementa las ventas al permitir una relación más estrecha con los clientes y los socios de negocios, a través de comunicaciones seguras y procesos colaborativos.Por otra parte, si el criterio de que la seguridad se ocupa de la protección de los bienes, parece natural establecer cuáles son los bienes informáticos a proteger. A primera vista, puede decirse que estos son: el hardware; el software y los datos. Entre ellos, los más expuestos a riesgos, son los datos. Se devalúan rápidamente, su tiempo de vida útil suele ser corto y pierden su valor antes que el hardware, cuyo tiempo de vida se estima en 2 ó 3 años, y el software, que en ocasiones, con los mantenimientos oportunos, pueden operar durante más de 5 años. (RODRÍGUEZ, 2000)
- Amenazas más sutiles provienen de los controles inadecuados de la programación, como es el problema de los residuos, es decir, de la permanencia de información en memoria principal cuando un usuario la libera o, en el caso de dispositivos externos, cuando se borra incorrectamente. Una técnica fraudulenta muy utilizada consiste en transferir información de un programa a otro mediante canales ilícitos, no convencionales (canales ocultos). El análisis del comportamiento de las amenazas a la seguridad de la información revela que la mayoría de los hechos se cometen por intrusos individuales. Un por ciento menor corresponde a

incidentes protagonizados por grupos organizados, y en la punta de la pirámide, se ubican los casos de espionaje (industrial, económico, militar...). (ÁNGEL, 2003)

Según la Oficina de Ciencia y Tecnología de la Casa Blanca, las pérdidas anuales estimadas en Estados Unidos, debido al espionaje económico ascienden a 100 mil millones de dólares.

En Internet, las principales amenazas para la protección de la información provienen de:

- Anexos a mensajes enviados por correo electrónico infectados con virus.
- El intercambio de códigos de virus.
- Firewalls o cortafuegos mal configurados.
- Ataques a la disponibilidad de los recursos de información existentes en la red (bancos de datos o software disponibles para descargar por los usuarios).
- La alteración de las páginas web.
- El "repudio" y las estafas asociadas al comercio electrónico.
- Las vulnerabilidades de los sistemas operativos y la desactualización de los "parches" concernientes a su seguridad.
- La rotura de contraseñas.
- La suplantación de identidades.
- El acceso a páginas pornográficas, terroristas, etc.
- El robo y la destrucción de información.
- Pérdida de tiempo durante el acceso a sitios ajenos a la razón social de la entidad.
- El hecho de que herramientas de hacking y cracking se ofrezcan como freeware.

Por estas y otras razones, el tratamiento de los temas relacionados con la seguridad informática ha tomado un gran auge.

Los problemas relacionados con la confidencialidad, integridad y autenticidad en un documento electrónico se resuelven mediante la tecnología llamada Criptografía. (INFORMATION SYSTEMS AUDIT, 2012)

Materiales y métodos

Se realizó una revisión selectiva sobre el tema objeto de estudio. La consulta se efectuó en dos niveles: primero, desde la perspectiva de la seguridad informática en general y segundo, dirigida particularmente al tema de la Criptografía de esta manera se obtuvo una gran cantidad de documentos generales y específicos que permitieron ubicar y comprender mejor al objeto de estudio particular: la Criptografía, en el contexto de la seguridad informática.

Discusión

La Criptografía es una rama de las matemáticas que, al orientarse al mundo de los mensajes digitales, proporciona las herramientas idóneas para solucionar los problemas relacionados con la autenticidad y la confiabilidad. El problema de la confidencialidad se vincula comúnmente con técnicas denominadas de "encripción" y la autenticidad con técnicas denominadas de "firma digital", aunque la solución de ambos, en realidad, se reduce a la aplicación de procedimientos criptográficos de encripción y descripción. (MENDVIL, 2003)

El Criptoanálisis es la ciencia que se ocupa del análisis de un texto cifrado para obtener la información original sin conocimiento de la clave secreta, esto es, de forma ilícita rompiendo así los

procedimientos de cifrado establecidos por la Criptografía, por lo que se dice que Criptoanálisis y Criptografía son ciencias complementarias pero contrarias. (ANGEL, 2003)

El uso de técnicas criptográficas tiene como propósito prevenir algunas faltas de seguridad en un sistema computarizado.

La seguridad, en general, se considera como un aspecto de gran importancia en cualquier corporación que trabaje con sistemas computarizados. El hecho de que gran parte de actividades humanas sean cada vez más dependientes de los sistemas computarizados, hace que la seguridad desempeñe una función protagónica. (MENEZES ,2009)

Otros autores plantean que la Criptografía se ocupa del problema de enviar información confidencial por un medio inseguro. Para garantizar la confidencialidad, podría asegurarse el medio de transmisión o bien la información; la Criptografía utiliza este último enfoque, encripta la información de manera que, aun cuando se encuentre disponible para cualquiera, no pueda utilizarla, a menos que alguien autorizado la descifre. (MENEZES ,2009)

La diferencia entre Criptografía y seguridad informática puede ilustrarse así:

En un modelo criptográfico típico, existen dos puntos: "a" y "b", que se consideran fiables y, entre ellos, se transmite información mediante un canal no fiable. La Criptografía se ocupa de los problemas relacionados con la transmisión confidencial y segura por el medio no fiable, en tanto la seguridad informática se ocupa de asegurar la fiabilidad de los nodos "a" y "b". (ANGEL, 2003)

La Criptografía se divide en dos grandes ramas, la Criptografía de clave privada o simétrica y la Criptografía de clave pública o asimétrica. La primera se refiere al conjunto de métodos que permiten una comunicación segura entre las partes siempre que, con anterioridad, se intercambie la

clave correspondiente, que se denomina clave simétrica. La simetría se refiere a que las partes tienen la misma llave, tanto para cifrar como para descifrar. (ANGEL, 2003)

La Criptografía simétrica, se ha implementado en diferentes tipos de dispositivos: manuales, mecánicos, eléctricos, hasta llegar a las computadoras, donde se programan los algoritmos actuales. La idea general es aplicar diferentes funciones al mensaje que se desea cifrar de modo tal, que sólo conociendo la clave, pueda descifrarse. Aunque no existe un tipo de diseño estándar, tal vez, el más popular es el de Fiestel, que realiza un número finito de interacciones de una manera particular, hasta que finalmente el mensaje es cifrado. Este es el caso del sistema criptográfico simétrico más conocido: DES (Data Encryption Standard). (ANGEL, 2003)

Este último, el DES, es un sistema criptográfico que toma como entrada un bloque de 64 bits del mensaje y lo somete a 16 interacciones. Su clave de 56 bits, en la práctica tiene 64 bits, porque a cada conjunto de 7 bits se le agrega un bit que puede utilizarse para establecer la paridad. DES tiene 4 modos de operación: ECB (Electronic Codebook Mode) para mensajes cortos, de menos de 64 bits, CBC (Cipher Block Chaining Mode) para mensajes largos, CFB (Cipher Block Feedback) para cifrar bit por bit o byte por byte y el OFB (Output Feedback Mode) con el mismo uso, pero que evita la propagación de errores. (FEDERAL INFORMATION, 2010)

Hasta el momento, no se ha podido romper el sistema DES mediante la deducción de la clave simétrica a partir de la información interceptada; sin embargo, con un método de fuerza bruta, la prueba de alrededor de 256 posibles claves, pudo descifrarse DES en enero de 1999. Ello implica que, es posible obtener la clave del sistema DES en un tiempo relativamente corto; así, se ha vuelto inseguro para propósitos de alta seguridad. La opción que se ha tomado para sustituir a DES es el cifrado múltiple, que aplica varias veces el mismo algoritmo para fortalecer la longitud de la clave y

que ha tomado forma como nuevo sistema para el cifrado y se conoce actualmente como triple-DES o TDES. (FEDERAL INFORMATION, 2010)

La Criptografía de clave pública o asimétrica, también denominada RSA por las siglas de los apellidos de sus inventores Rivest Shamir y Adelman, es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la Criptografía asimétrica ocurrió como resultado de la búsqueda de un modo más práctico de intercambiar las llaves simétricas. (Bradanovic, 2004)

Los algoritmos criptográficos tienden a degradarse con el tiempo. A medida que transcurre el tiempo, los algoritmos de encripción se hacen más fáciles de quebrar debido al avance de la velocidad y potencia de los equipos de computación. (ANGEL, 2003)

Todos los algoritmos criptográficos son vulnerables a los ataques de fuerza bruta -tratar sistemáticamente con cada posible clave de encripción, buscando colisiones para funciones hash, factorizando grandes números, etc.- la fuerza bruta es más fácil de aplicar en la medida que pasa el tiempo. (ANGEL, 2003)

Las vulnerabilidades en los sistemas de información pueden traer graves problemas. Cada vez las redes están expuestas a virus informáticos, spam, código malicioso, hackers y crakers que penetran los sistemas de seguridad. Los elementos que la seguridad de la información busca proteger son:

- La información
- Los equipos que la soportan
- Las personas que la utilizan

El primero de los tres principios de la seguridad de la información que aplicamos es la integridad, la cual nos permite garantizar que la información no ha sido alterada en su contenido, por tanto, es íntegra. El principio de la confidencialidad de la información tiene como propósito el asegurar que sólo la persona correcta acceda a la información que queremos distribuir. (INFORMATION SYSTEMS AUDIT, 2012)

Una vez que nos aseguramos que la información correcta llegue a los destinatarios o usuarios correctos, ahora lo que debemos garantizar es que llegue en el momento oportuno, y precisamente de esto trata el tercer principio de la seguridad de la información: la disponibilidad. Para que una información se pueda utilizar, deberá estar disponible. (INFORMATION SYSTEMS AUDIT, 2012)

Es importante, además, que todos los empleados de la compañía tomen conciencia sobre el manejo de la información de forma segura, ya que de nada sirve cualquier sistema de seguridad, por complejo y completo que este sea, si los empleados, por ejemplo, facilitan su usuario y contraseña a personas ajenas a la empresa y con esto dejan abierta la puerta a posibles ataques o filtraciones de información crítica al exterior de la compañía. (MENDVIL, 2003)

El análisis y evaluación de riesgos permite a las compañías tener una visión más clara sobre sus vulnerabilidades y de los esfuerzos que deben hacer para mejorar.

En el mundo de las certificaciones de calidad y en el cumplimiento de estándares internacionales que permitan acceder a nuevos mercados o se brinden nuevos valores agregados que marquen una diferenciación o ventaja competitiva, las políticas definen la forma de hacer las cosas, el mejoramiento de los procesos. Reconocer las limitaciones y restricciones de la tecnología es un buen paso para entender la importancia de las políticas. En este sentido podemos definir la política como un instrumento gerencial que traza una dirección predeterminada describiendo la manera de

manejar un problema o situación. Las políticas son planteamientos de alto nivel que transmiten a los colaboradores de la empresa la orientación que necesitan para tomar decisiones presentes y futuras. (MENDVIL, 2003)

Conclusiones.

Las políticas deben ser claras, concisas, contextualizadas a una realidad, enfocadas a las forma de hacer negocios de la empresa. Según las cifras presentadas en estudios relacionados con seguridad informática en las empresas más de un 60% de las compañías no cuenta con programas establecidos de seguridad informática. Debido a las cambiantes condiciones y nuevas plataformas de computación disponibles, es vital el desarrollo de documentos y directrices que orienten a los usuarios en el uso adecuado de las tecnologías para aprovechar mejor sus ventajas. (INFORMATION SYSTEMS AUDIT, 2012)

El auge de la interconexión entre redes abre nuevos horizontes para la navegación por Internet y con ello, surgen nuevas amenazas para los sistemas computarizados, como son la pérdida de confidencialidad y autenticidad de los documentos electrónicos. (RODRÍGUEZ, 2000)

La Criptografía es una disciplina/tecnología orientada a la solución de los problemas relacionados con la autenticidad y la confidencialidad, y provee las herramientas idóneas para ello. Los usuarios son quienes deben elegir la conveniencia de una u otra herramienta para la protección de sus documentos electrónicos. (RODRÍGUEZ, 2000)

Recomendaciones

No obstante, las políticas de seguridad, los procedimientos, los controles y las medidas de seguridad de los activos informáticos manteniendo siempre así un nivel de seguridad adecuado y

una administración del riesgo razonable; todo ello a un costo proporcional y razonable al valor de los bienes informáticos guardados y por lo tanto se deben considerar ciertos elementos tales como:

Algunas de las recomendaciones puntuales a este propósito:

- Invertir en los avances en el área de tecnología, es esencial para que la criptografía tome ventaja ante los ataques cibernéticos. Esos nuevos recursos realizan las soluciones de seguridad más alineadas y compatibles con los padrones más recientes de criptografía.
- Revisar periódicamente mediante un plan al efecto las normas, políticas, procedimientos y controles de la seguridad informática para perfeccionarlos y mantenerlos actualizados.
- Consolidar un grupo o comité oficial de seguridad informática con personas, funciones y responsabilidades perfectamente establecidas.
- De los inventarios, auditorías, bitácoras, etcétera se obtienen siempre mediciones acerca de algunas estrategias y controles que siempre faltan de implementar en toda organización o que deben perfeccionarse; debe hacerse una revisión equivalente para evaluar los riesgos y actuar al efecto.
- Establecer los dominios de acción y objetivos que no satisfagan del todo a lo estipulado por la organización e incidir con mayor rigor en ellos. (GRANGER, 2009)

Finalmente, es importante que señalar que podemos diseñar entornos de seguridad informática para cualquier organización que no necesariamente requerimos que desemboquen en la preservación de archivos digitales a largo plazo, pero no podemos, –y no debemos– diseñar y construir ambientes de preservación de archivos digitales a largo plazo sin contemplar en ese proyecto y desde el principio la seguridad informática de la organización. (GRANGER, 2009)

Bibliografía

1. Angel Angel JJ. Criptografía para principiantes. (15 de enero de 2003): http://www.htmlweb.net/seguridad/cripto_p/cripto_princ_1.html, Recuperado: 14 de enero del 2018.

2. Bradanovic T. Algo sobre Criptografía. (20 de enero del 2004) http://www.vcd.cl/tombrad/pcasual/ayuda5.html, Recuperado: 14 de enero del 2018.

3. Aneiro Rodríguez LO. Elementos de arquitectura y seguridad informática. La Habana: Instituto Superior Politécnico "Eduardo García Delgado", 2000.

4. Menezes AJ, Oorschot PC, Vanstone SA. Handbook of applied Cryptography. (10 de febrero del 2003) http://www.cacr.math.uwaterloo.ca/hac/, Recuperado: 14 de enero del 2018.

5. Federal Information Processing Standards. FIPS 81. DES modes of operation (24 de febrero del 2010). Disponible en: http://www.itl.nist.gov/fipspubs/fip81.htm ,Recuperado: 14 de enero del 2018.

6. Mendvil I. El ABC de los documentos electrónicos seguros (20 de enero del 2003). http://www.criptored.upm.es/guiateoria/gt_m163a.htm, Recuperado:. 14 de enero del 2018.

7. INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION Estándares de Seguridad, ISACA, IEC/ISO (20 de enero del 2012), http://www.isaca..org, Recuperado: 14 de enero del 2018.

8. Granger, Sarah. 2009. "Social Engineering Fundamentals, Part I: Hacker Tactics". Security Focus. (19 noviembre, 2009), en: http://www.securityfocus.com/infocus/1527, Recuperado: 14 de enero del 2018.